PFJA-01015C-US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ３月１３日

出願番号
Application Number: 特願２００１－０７１２１４

[ST.10/C]: [ＪＰ２００１－０７１２１４]

出願人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００２年 １月１８日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００１－３１１７３４９

【書類名】　特許願

【整理番号】　0150025

【提出日】　平成13年 3月13日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/00

G06F 13/00

【発明の名称】　フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム

【請求項の数】　9

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　三友　仁史

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　鳥居　悟

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　滝沢　文恵

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小野　越夫

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷野　修

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100089118

【弁理士】

【氏名又は名称】　酒井　宏明

【手数料の表示】

【予納台帳番号】　036711

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9717671

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム

【特許請求の範囲】

【請求項１】　クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積手段と、

前記見積手段による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定手段と、

を備えたことを特徴とするフィルタリング装置。

【請求項２】　前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記判定手段は、前記見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする請求項１に記載のフィルタリング装置。

【請求項３】　前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記判定手段は、前記見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする請求項１に記載のフィルタリング装置。

【請求項４】　前記サーバに対する正当アクセスのパターンを格納した正当

パターンデータベースと、前記見積手段による正当性の見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする請求項１、２または３に記載のフィルタリング装置。

【請求項５】　所定の外部送信ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する外部送信手段をさらに備えたことを特徴とする請求項１～４のいずれか一つに記載のフィルタリング装置。

【請求項６】　所定の格納ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する格納手段をさらに備えたことを特徴とする請求項１～５のいずれか一つに記載のフィルタリング装置。

【請求項７】　所定の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新する更新手段をさらに備えたことを特徴とする請求項１～６のいずれか一つに記載のフィルタリング装置。

【請求項８】　クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス要求のみを受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

を含んだことを特徴とするフィルタリング方法。

【請求項９】　クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス

要求のみを受け渡すフィルタリング方法をコンピュータに実行させるプログラムにおいて、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムに関する。

【０００２】

近時、ネットワーク技術の進展に伴って、インターネット上の分散システムであるＷＷＷ（World Wide Web）の利用が急速に拡大し、クライアントからの各種のリクエスト（アクセス要求）に応じて各種のサービスを提供する各種ＨＴＴＰサーバも累増してきたが、かかるサーバの累増にともなって、クライアントによるサーバへの不正アクセスも増加しつつある。

【０００３】

すなわち、侵入者（イントルーダ）や攻撃者（アタッカ）が企業、団体、個人などのサーバを無権限で不正に利用したり、運用を妨害したり、破壊（クラック）など、サーバを利用する者がその者に与えられた権限により許された行為以外の行為をネットワークを介して意図的におこなうという不正アクセスが増加している。このため、サーバに対する不正アクセスを拒絶することによりサーバの信頼性を確保する必要性が高まりつつある。

【０００４】

【従来の技術】

従来より、クライアントによる不正アクセスからサーバを守るために、インターネットと企業ＬＡＮ（Local Area Network）との間にファイアウォール（Fire Wall）を構築することが一般的におこなわれている。

【０００５】

このファイアウォールは、インターネットに接続したコンピューターやネットワークへの外部からの侵入を防ぐためのソフトウエアであり、企業ＬＡＮとインターネットの間に、特定のデータやプロトコルだけを通すように設計されたファイアウォール用のコンピュータを置き、ＬＡＮ内と外部とのデータ交換はすべてこのマシンを通しておこなうことにより、外部からの侵入を防ぐというものである。

【０００６】

また、このファイアウォールに関連して、ネットワークベースあるいはホストベースの不正アクセス検知手法がある。前者のネットワークベースの不正アクセス検知手法は、ネットワークを流れる生のパケットを監視することにより不正アクセスを発見するものであり、後者のホストベースの不正アクセス検知手法は、ホストに蓄えられたログ履歴を監視することにより不正アクセスを発見するものである。

【０００７】

そして、このような不正アクセス検知手法により発見された不正アクセスに基づいて不正アクセスの送信元クライアントを突き止め、この不正アクセスをおこなったクライアントのＩＰアドレスなどの送信元情報をファイアウォール用のコンピュータ内に蓄積することにより、この送信元情報を含んだクライアントからのアクセス要求を不正アクセスとして拒絶することがファイアウォールにおいて一般的におこなわれている。

【０００８】

【発明が解決しようとする課題】

しかしながら、上記の従来技術は、過去に不正アクセスをおこなったクライアントを不正クライアントと認定し、この不正クライアントからのアクセス要求を

不正アクセスとして拒絶するものであるため、不正クライアントと認定された後の不正アクセスに対してはサーバを防御することができるが、不正クライアントと認定されていないクライアントからの不正アクセスに対してはサーバを防御することができないという問題点があった。すなわち、不正クライアントと認定される前の初回の不正アクセスに対してはサーバを防御することができない。

【０００９】

このため、不正クライアントと認定されていないクライアントからの不正アクセスに対していかにサーバを防御するかが極めて重要な課題となっており、望ましくは、アクセス要求の送信元情報を考慮することなく、正当なアクセス要求であるか不正なアクセス要求であるか否かを判定する枠組みが必要とされている。

【００１０】

そこで、この発明は、上述した従来技術による問題点を解消するためになされたものであり、不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができるフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムを提供することを目的とする。

【００１１】

【課題を解決するための手段】

上述した課題を解決し、目的を達成するため、請求項１、８または９の発明によれば、図１に示す見積部３２は、Ｗｅｂサーバ４０に対する不正アクセスのパターンを格納した不正リクエストＤＢ（データベース）３３を参照し、不正アクセスのパターンおよび所定の見積ルール３２ａに基づいてクライアント装置１０からのアクセス要求の正当性を見積もり、判定部３４は、見積部３２による見積結果および所定の判定ルール３４ａに基づいてアクセス要求をＷｅｂサーバ４０に受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみをＷｅｂサーバ４０に受け渡すことができ、もって不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対してもＷｅｂサーバ４０を防御することができ

る。

【００１２】

また、請求項２の発明によれば、図１に示す見積部３２は、クライアント装置１０からのアクセス要求が不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、クライアント装置１０からのアクセス要求が不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、判定部３４は、見積部３２により不正アクセスである旨が見積もられたアクセス要求をＷｅｂサーバ４０に受け渡さないものと判定するとともに、見積部３２により正当アクセスである旨が見積もられたアクセス要求をＷｅｂサーバ４０に受け渡すものと判定することとしたので、アクセス要求が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対しても迅速かつ確実にＷｅｂサーバ４０を防御することができる。

【００１３】

また、請求項３の発明によれば、図１に示す見積部３２は、クライアント装置１０からのアクセス要求が不正リクエストＤＢ３３に格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、判定部３４は、見積部３２により算出された見積値と所定の閾値とを比較してアクセス要求をＷｅｂサーバ４０に受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対してもある程度の幅を持ってＷｅｂサーバ４０を防御することができる。

【００１４】

また、請求項４の発明によれば、図５に示す事前判定部７１は、見積部３２による正当性の見積もりの前に、Ｗｅｂサーバ４０に対する正当アクセスのパターンを格納した正当リクエストＤＢ７２を参照し、クライアント装置１０からのア

クセス要求が正当リクエストＤＢ７２に格納された正当アクセスのパターンのいずれかに該当するか否かを判定し、見積部３２は、事前判定部７１により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなくＷｅｂサーバ４０に受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

【００１５】

また、請求項５の発明によれば、図１に示す外部通報部３７は、所定の通報ルール３７ａに基づいて、判定部３４によりＷｅｂサーバ４０に受け渡さないものと判定されたアクセス要求を所定の外部装置５０に送信することとしたので、不正アクセスに関する情報をＷｅｂサーバ４０の管理者、リクエストフィルタ３０の管理者、サーバ装置２０全体の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に通報することができ、もってかかる管理者に対しＷｅｂサーバ４０の保全対策を迅速に促すことができる。

【００１６】

また、請求項６の発明によれば、図１に示すログ管理部３６は、所定の管理ルール３６ａに基づいて、判定部３４によりＷｅｂサーバ４０に受け渡さないものと判定されたアクセス要求を所定の格納媒体３６ｂに格納することとしたので、格納媒体３６ｂに格納された不正アクセスに関する情報を分析することなどができ、もってＷｅｂサーバ４０の更なる保全対策を講じることができる。

【００１７】

また、請求項７の発明によれば、図１に示す更新部３９は、所定の更新ルール３９ａに基づいて、不正リクエストＤＢ３３、正当リクエストＤＢ７２（図５に示す）、見積ルール３２ａ、判定ルール３４ａ、通報ルール３７ａ、管理ルール３６ａまたは更新ルール３９ａを更新することとしたので、新たに発見された不正アクセスのパターンを不正リクエストＤＢ３３に登録することなどができ、もって日々進化する不正アクセスに対して機動的に対応することができる。

【００１８】

【発明の実施の形態】

以下に添付図面を参照して、この発明に係るフィルタリング装置、フィルタリング方法、およびその方法をコンピュータに実行させるプログラムの好適な実施の形態を詳細に説明する。なお、以下に示す実施の形態１～３では、本発明に係るフィルタリング技術を、クライアント装置からのＨＴＴＰ（HyperText Transfer protocol）リクエストに応じてサービスを提供するサーバ装置に適用した場合について説明する。

【００１９】

（実施の形態１）

本実施の形態１では、クライアント装置からのＨＴＴＰリクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明する。

【００２０】

（１）システムの全体構成

まず最初に、本実施の形態１に係るクライアントサーバシステムの構成について説明する。図１は、本実施の形態１に係るクライアントサーバシステムの構成を示すブロック図である。同図に示すように、本実施の形態１に係るクライアントサーバシステムは、Ｗｅｂブラウザ１１をそれぞれ有する複数のクライアント装置１０と、フィルタリング装置としてのリクエストフィルタ３０およびＷｅｂサーバ４０を有するサーバ装置２０とを、インターネットなどのネットワーク１を介して相互に通信可能に接続して構成される。

【００２１】

概略的に、このクライアントサーバシステムにあっては、クライアント装置１０は、ブラウザ１１によりサーバ装置２０に対してＨＴＴＰリクエストなどの各種の処理要求をおこない、サーバ装置２０のＷｅｂサーバ４０は、クライアント装置１０からのＨＴＴＰリクエストに応じたサービスをクライアント装置１０に提供する。そして、サーバ装置２０のリクエストフィルタ３０は、クライアント装置１０とＷｅｂサーバ４０との間に介在し、クライアント装置１０からのＨＴ

ＴＰリクエストのうちの正当なリクエストのみをＷｅｂサーバ４０に受け渡す。

【００２２】

ここで、本実施の形態１に係るクライアントサーバシステムは、サーバ装置２０のリクエストフィルタ３０によるフィルタリング処理に特徴があり、具体的には、リクエストフィルタ３０の見積部３２は、クライアント装置１０からのＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれかに該当する場合には不正アクセスである旨を見積もり、判定部３４は、見積部３２により不正アクセスである旨が見積もられたＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定することにより、ＨＴＴＰリクエストの送信元情報を問題とすることなく、正当なＨＴＴＰリクエストのみをＷｅｂサーバ４０に受け渡すことができるように構成している。

【００２３】

（２）クライアント装置の構成

次に、図１に示したクライアント装置１０の構成について説明する。同図に示すように、クライアント装置１０は、Ｗｅｂブラウザ１１を備え、基本的には、サーバ装置２０に対してＨＴＴＰリクエストなどの処理要求をおこない、サーバ装置２０のＷｅｂサーバ４０により提供されるＷｅｂデータを解釈して、モニタなどの出力部に表示させる表示制御（ブラウズ処理）をおこなう。

【００２４】

そして、このクライアント装置１０は、悪意を持った使用方法によってサーバ装置２０に対して不正アクセスをおこなうことができる装置でもある。すなわち、クライアント装置１０は、侵入者（イントルーダ）や攻撃者（アタッカ）などの悪意を持ったユーザの使用によっては、Ｗｅｂサーバ４０上のパスワードファイルなどのリモートユーザが見るべきでないファイルを見たり、Ｗｅｂサーバ４０上に存在しないファイルをリクエストしてＷｅｂサーバ４０の機能を停止させたり、コマンド文字列を含んだリクエストによりＷｅｂサーバ４０上で任意のシステムコマンドを実行するなどの不正アクセスをおこない得るものである。このようなクライアント装置１０による不正アクセスに対してＷｅｂサーバ４０を防御するのがリクエストフィルタ３０の役割である。

【００２５】

なお、クライアント装置１０は、たとえば、パーソナルコンピュータやワークステーション、家庭用ゲーム機、インターネットＴＶ、ＰＤＡ(Personal Digital Assistant)、あるいは、携帯電話やＰＨＳ（Personal Handy Phone System）の如き移動体通信端末によって実現することができる。また、クライアント装置１０は、モデム、ＴＡ、ルータなどの通信装置と電話回線を介して、あるいは、専用線を介して、ネットワーク１に接続されており、所定の通信規約（たとえば、ＴＣＰ／ＩＰインターネットプロトコル）に従ってサーバ装置２０にアクセスすることができる。

【００２６】

（３）サーバ装置におけるＷｅｂサーバの構成

次に、図１に示したサーバ装置２０におけるＷｅｂサーバ４０の構成について説明する。同図に示すように、サーバ装置２０のＷｅｂサーバ４０は、リクエストフィルタ２０を介してクライアント装置１０からのＨＴＴＰリクエストを受信し、このＨＴＴＰリクエストに応じてＨＴＭＬ（HyperText Markup Language）などのマークアップ言語により記述された各種の情報を送信するなどのサービスをクライアント装置１０に提供する。

【００２７】

このＷｅｂサーバ４０は、機能概念的には、一般的なＷｅｂサーバと同様の動作をおこなうものであるが、ここでのＷｅｂサーバ４０は、一般的なＷｅｂサーバと異なり、サーバ装置２０においてＨＴＴＰリクエストに割り当てられるポート番号８０のＴＣＰ（Transmission Control Protocol）ポートを監視することはおこなわない。

【００２８】

すなわち、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０により直接に受信するのではなく、リクエストフィルタ３０がＨＴＴＰリクエストを受信し、プロセス間通信をおこなって正当なＨＴＴＰリクエストのみをＷｅｂサーバ４０に受け渡すこととしている。

【００２９】

（４）サーバ装置におけるリクエストフィルタの構成

次に、図１に示したサーバ装置２０におけるリクエストフィルタ３０の構成について説明する。同図に示すように、リクエストフィルタ３０は、受信部３１と、見積部３２と、不正リクエストＤＢ３３と、判定部３４と、送信部３５と、ログ管理部３６と、外部通報部３７と、外部情報取得部３８と、更新部３９とを備える。

【００３０】

このうち、受信部３１は、サーバ装置２０におけるポート番号８０のＴＣＰポートを監視して、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する処理部である。なお、受信部３１によりクライアント装置１０から受信したＨＴＴＰリクエストは、見積部３２および送信部３３に出力される。

【００３１】

見積部３２は、不正リクエストＤＢ３３に格納された不正アクセスのパターンおよび所定の見積ルール３２ａに基づいてＨＴＴＰリクエストの正当性を見積もり、その見積結果を判定部３４に出力する処理部である。

【００３２】

ここで、見積部３２が見積もりに際して参照する不正リクエストＤＢ３３について説明する。図２は、不正リクエストＤＢ３３に格納される情報の構成例を示す図である。同図に示すように、不正リクエストＤＢ３３は、サーバに対する不正アクセスのパターンを格納したデータベースであり、ネットワーク世界で収集された不正アクセスを図示のような形式言語を用いて記述した複数のパターンを記憶している。

【００３３】

例えば、同図に示す「ＵＲＬ＝＜／／」のパターンは、ＵＲＬ（Uniform Resource Locator）の先頭が「／／」である不正リクエストを意味し、「ＣＧＩ＝＝ｐｈｆ、ＡＲＧ＝＜Ｑｎａｍｅ＝ｒｏｏｔ％ＯＡ」のパターンは、ＣＧＩ（Common Gateway Interface）名が「ｐｈｆ」であり、そのある引数の先頭が「Ｑｎａｍｅ＝ｒｏｏｔ％ＯＡ」である不正リクエストを意味し、「ＵＲＬ＜＞．．

¥．．¥．．¥．．」のパターンは、ＵＲＬに「．．¥．．¥．．¥．．」が含まれる不正リクエストを意味し、「ＣＧＩ＞＝．ｈｔｒ」のパターンは、ＣＧＩ名の末尾が「．ｈｔｒ」である不正リクエストを意味する。

【００３４】

なお、図２には示していないが、不正リクエストＤＢ３３には、Ｗｅｂサーバ４０上で任意のシステムコマンドを実行するような不正なコマンド文字列も複数記憶されている。このようなコマンド文字列のパターンを記憶することにより、攻撃方法が既知である不正アクセスだけでなく、攻撃方法が未知である不正アクセスに対してもＷｅｂサーバ４０を防御することができる。

【００３５】

このような不正リクエストＤＢ３３を参照することにより、見積部３２は、所定の見積ルール３２ａに基づいてＨＴＴＰリクエストの正当性の見積もりをおこなう。具体的には、ＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれかに該当する場合には、該ＨＴＴＰリクエストは不正アクセスである旨を見積もり、一方、ＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれにも該当しない場合には、該ＨＴＴＰリクエストは正当アクセスである旨を見積もる。

【００３６】

図１の説明に戻ると、判定部３４は、見積部３２から受け取った見積結果および所定の判定ルール３４ａに基づいてＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定し、この判定結果を送信部３５に出力する処理部である。具体的には、見積部３２から不正アクセスである旨の見積結果を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定し（不可判定）、一方、見積部３２から正当アクセスである旨の見積結果を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すものと判定する（可判定）。

【００３７】

送信部３５は、判定部３４から受け取った判定結果に基づいて、受信部３１から受け取ったＨＴＴＰリクエストの送信を制御する処理部である。具体的には、

判定部３４から可判定を受け取った場合には、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡す。一方、判定部３４から不可判定を受け取った場合には、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶して、この不正リクエストを破棄する。

【００３８】

ログ管理部３６は、所定の管理ルール３６ａに基づいて、判定部３４によりＷｅｂサーバ４０に受け渡さないものと判定された不正リクエストに係る情報を格納媒体３６ｂに格納して管理する処理部である。具体的には、管理ルール３６ａに基づいて、不正リクエストの内容、送信元情報（ＩＰアドレスやホスト名）、送信時刻、見積部３２による見積結果の根拠、判定部３４による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に格納媒体３６ｂに格納する。例えば、攻撃性の高い不正リクエストのみを格納するなどである。

【００３９】

なお、格納媒体３６ｂに格納された情報は、該格納媒体３６ｂを取り出すことや通信回線を介することなどによりサーバ装置２０の外部に出力することができ、さらに、格納媒体３６ｂに格納された情報を分析して不正アクセスの傾向などを解析することにより、Ｗｅｂサーバ４０の更なる保全のために対策を講じることもできる。

【００４０】

外部通報部３７は、所定の通報ルール３７ａに基づいて、判定部３４によりＷｅｂサーバ４０に受け渡さないものと判定された不正リクエストに係る情報を外部装置５０に通報する処理部である。具体的には、ログ管理部３６による処理と同様、通報ルール３７ａに基づいて、不正リクエストの内容、送信元情報（ＩＰアドレスやホスト名）、送信時刻、見積部３２による見積結果の根拠、判定部３４による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に外部装置５０に通報する。

【００４１】

この外部通報部３８から通報を受ける外部装置５０は、Ｗｅｂサーバ４０の管理者、リクエストフィルタ３０の管理者、サーバ装置２０全体の管理者、ネットワーク全般を監視する公的な機関（管理センタ）の管理者など（以下、これらを総称して「管理者」という。）が操作する通信装置である。そして、外部通報部３７は、例えば、攻撃性の高い不正リクエストについてはリアルタイムで迅速に管理者に通報し、攻撃性の低い不正リクエストについては非リアルタイムで一括して管理者に通報するなどして、かかる通報を受ける管理者に対してＷｅｂサーバ４０の保全対策を迅速に促すことができる。

【００４２】

外部情報取得部３８は、所定の取得ルール３８ａに基づいて、更新部３９による更新処理に用いられる情報を、外部装置５０やＷｅｂサーバ４０などのリクエストフィルタ３０の外部から能動的または受動的に取得する処理部である。例えば、管理者が外部装置５０を介して入力した新たな不正リクエストのパターンや、管理者が外部装置５０を介して入力した見積ルール３２ａの変更指示情報などを取得するほか、不正リクエストによる被害を受けたＷｅｂサーバ４０から被害の状況や不正アクセスの内容などの情報を取得する。なお、所定の取得ルール３８ａは、権限が認証された管理者からの情報のみを取得するなどの規則である。

【００４３】

更新部３９は、所定の更新ルール３９ａに基づいて、不正リクエストＤＢ３３、見積ルール３２ａ、判定ルール３４ａ、管理ルール３６ａ、通報ルール３７ａ、取得ルール３８ａまたは更新ルールに格納された情報を更新する処理部である。例えば、外部情報取得部３８から新たな不正リクエストのパターンを受け付けた場合には、この不正リクエストのパターンを不正リクエストＤＢ３３に格納し、また見積ルール３２ａの変更指示情報を受け付けた場合には、この変更指示情報に応じて見積ルール３２ａを変更する。このような更新処理をおこなうことにより、日々進化する不正アクセスに対して機動的に対応することができる。

【００４４】

（５）フィルタリング処理

次に、本実施の形態１によるフィルタリングの処理手順について説明する。図

３は、本実施の形態１によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置２０におけるリクエストフィルタ３０の受信部３１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する（ステップＳ３０１）。

【００４５】

そして、リクエストフィルタ３０の見積部３２は、不正リクエストＤＢ３３に格納された不正アクセスのパターンおよび所定の見積ルール３２ａに基づいてＨＴＴＰリクエストの正当性を見積もる（ステップＳ３０２）。具体的には、ＨＴＴＰリクエストが不正アクセスのパターンのいずれかに該当する場合には、不正リクエストである旨を見積もり、一方、ＨＴＴＰリクエストが不正アクセスのパターンのいずれにも該当しない場合には、正当リクエストである旨を見積もる。

【００４６】

その後、リクエストフィルタ３０の判定部３４は、見積部３２から受け取った見積結果および所定の判定ルール３４ａに基づいてＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定する（ステップＳ３０３）。具体的には、見積部３２により正当なリクエストである旨が見積もられたか否かを判定する。

【００４７】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップＳ３０３肯定）、リクエストフィルタ３０の送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡し（ステップＳ３０４）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じた情報をクライアント装置１０に送信するなどの正当判定時の処理をおこなう（ステップＳ３０５）。

【００４８】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップＳ３０３否定）、リクエストフィルタ３０の送信部３５は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶し（ステップＳ３０６）、リクエストフィルタ３０の各部は、不正リクエストの破棄、格納媒体３６ｂへの格納、外部装置５０への通報などの不正判定時の処理をおこなう（ステッ

プＳ３０７）。

【００４９】

上述してきたように、本実施の形態１によれば、アクセス要求の送信元情報ではなく、アクセス要求の具体的な要求内容が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができる。これにより、不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対しても迅速かつ確実にＷｅｂサーバ４０を防御することができる。

【００５０】

（実施の形態２）

ところで、上記実施の形態１では、クライアント装置からのＨＴＴＰリクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、ＨＴＴＰリクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合についても同様に適用することができる。

【００５１】

そこで、本実施の形態２では、ＨＴＴＰリクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合について説明する。なお、本実施の形態２においては、クライアントサーバシステムのシステム構成は図１に示すものと同様のものとなるので、ここではその詳細な説明を省略する。

【００５２】

まず最初に、本実施の形態２の特徴部分である見積部３２および判定部３４について説明する。本実施の形態２における見積部３２は、クライアント装置１０からのＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、その見積値を判定部３４に出力する。

【００５３】

具体的には、不正アクセスのパターンから一致するパターンの個数を算出する

ことや、各パターンに危険度数を付与して一致するパターンの危険度数を算出することなどにより、ＨＴＴＰリクエストの危険度を示すＤＩ（Danger　Index）と呼ばれる見積値を算出する。なお、見積値ＤＩは、例えば１～１００の範囲で整数値をとり、危険度が高いＨＴＴＰリクエストほど大きな値が算出されるというものである。

【００５４】

本実施の形態２における判定部３４は、見積部３２により算出された見積値ＤＩと所定の閾値とを比較してＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定し、この判定結果を送信部３５に出力する。

【００５５】

具体的には、所定の閾値を５０と仮定すると、見積部３２からＤＩが５０以上である見積値を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定し（不可判定）、一方、見積部３２からＤＩが５０未満である見積値を受け取った場合には、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すものと判定する（可判定）。

【００５６】

次に、本実施の形態２によるフィルタリングの処理手順について説明する。図４は、本実施の形態２によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置２０におけるリクエストフィルタ３０の受信部３１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する（ステップＳ４０１）。

【００５７】

そして、リクエストフィルタ３０の見積部３２は、ＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンに該当する度合に応じて見積値ＤＩを算出する（ステップＳ４０２）。リクエストフィルタ３０の判定部３４は、見積部３２により算出された見積値ＤＩと所定の閾値とを比較してＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定する（ステップＳ４０３）。具体的には、見積値ＤＩが所定の閾値以上であるか否かを判定する。

【００５８】

この判定により、見積値ＤＩが所定の閾値未満であると判定された場合には（ステップＳ４０３肯定）、リクエストフィルタ３０の送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡し（ステップＳ４０４）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じた情報をクライアント装置１０に送信するなどの正当判定時の処理をおこなう（ステップＳ４０５）。

【００５９】

これとは反対に、見積値ＤＩが所定の閾値以上であると判定された場合には（ステップＳ４０３否定）、リクエストフィルタ３０の送信部３５は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶し（ステップＳ４０６）、リクエストフィルタ３０の各部は、不正リクエストの破棄、格納媒体３６ｂへの格納、外部装置５０への通報などの不正判定時の処理をおこなう（ステップＳ４０７）。

【００６０】

上述してきたように、本実施の形態２によれば、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができる。これにより、不正クライアントと認定されていないクライアント装置１０からの不正アクセスに対してもある程度の幅を持ってＷｅｂサーバ４０を防御することができる。

【００６１】

（実施の形態３）

ところで、上記実施の形態１および２では、クライアント装置からの全てのＨＴＴＰリクエストについて不正アクセスのパターンに基づく見積もりをおこなう場合について説明したが、本発明にはこれに限定されるものではなく、一部のＨＴＴＰリクエストについてのみ見積もりをおこなう場合についても同様に適用することができる。

【００６２】

そこで、本実施の形態３では、二階層からなるフィルタリング処理をおこない、一部のＨＴＴＰリクエストについてのみ不正アクセスのパターンに基づく見積もりをおこなう場合について説明する。

【００６３】

図５は、本実施の形態３に係るクライアントサーバシステムの構成を示すブロック図である。なお、図１に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態３の特徴部分である事前判定部７１および正当リクエストＤＢ７２について説明する。

【００６４】

サーバ装置６０におけるリクエストフィルタ７０の事前判定部７１は、見積部３２による正当性の見積もりの前に、正当リクエストＤＢ７２に格納された正当アクセスのパターンおよび所定の事前判定ルール７１ａに基づいてＨＴＴＰリクエストの見積もりを省くことができるか否かを判定する処理部である。

【００６５】

ここで、事前判定部７１が判定に際して参照する正当リクエストＤＢ７２について説明すると、この正当リクエストＤＢ７２は、Ｗｅｂサーバ４０に対する正当アクセスのパターンを格納したデータベースであり、具体的には、Ｗｅｂサーバ４０上に存在するファイルのうちでリモートユーザに見られても構わないファイルのパスを記憶する。

【００６６】

このリモートユーザに見られても構わないファイルとは、パスワードファイルなどのリモートユーザが見るべきでないファイル以外のファイルであって、例えば、Ｗｅｂサーバ４０に対するＨＴＴＰリクエストのリクエスト内容として非常に高い割合を有する画像ファイルなど、不正アクセスの可能性がほとんどないようなファイルが含まれる。

【００６７】

このような正当リクエストＤＢ７２を参照することにより、事前判定部７１は、所定の事前判定ルール７１ａに基づいてＨＴＴＰリクエストの見積もりを省くことができるか否かを判定する。具体的には、ＨＴＴＰリクエストが正当リクエストＤＢ７２に格納された正当アクセスのパターンのいずれかに該当する場合には、該ＨＴＴＰリクエストの見積もりを省くことができるものと判定し、一方、ＨＴＴＰリクエストが正当リクエストＤＢ７２に格納された正当アクセスのパタ

ーンのいずれにも該当しない場合には、該ＨＴＴＰリクエストの見積もりを省くことができないものと判定する。

【００６８】

そして、事前判定部７１は、見積もりを省くことができないものと判定されたＨＴＴＰリクエストのみを見積部３２に出力し、見積もりを省くことができるものと判定されたＨＴＴＰリクエストについては、見積部３２および判定部３４による処理を省いて、送信部３５を介してＷｅｂサーバ４０に受け渡す。

【００６９】

なお、正当リクエストＤＢ７２に格納される正当アクセスのパターンは、Ｗｅｂサーバ４０に新たな画像ファイルが追加された場合などに応じて、更新部３９により更新される。

【００７０】

次に、本実施の形態３によるフィルタリングの処理手順について説明する。図６は、本実施の形態３によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置６０におけるリクエストフィルタ７０の受信部３１は、クライアント装置１０からのＨＴＴＰリクエストをＷｅｂサーバ４０が受信する前に受信する（ステップＳ６０１）。

【００７１】

そして、リクエストフィルタ７０の事前判定部７１は、正当リクエストＤＢ７２に格納された正当アクセスのパターンおよび所定の事前判定ルール７１ａに基づいてＨＴＴＰリクエストの見積もりを省くことができるか否かを判定する（ステップＳ６０２）。具体的には、ＨＴＴＰリクエストが正当リクエストＤＢ７２に格納された正当アクセスのパターンのいずれかに該当するか否かを判定する。

【００７２】

この判定により、正当アクセスのパターンのいずれかに該当するものと判定された場合には（ステップＳ６０２肯定）、このＨＴＴＰリクエストの正当性の見積もりを省き、リクエストフィルタ７０の送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡し（ステップＳ６０５）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じた情報をクライアント装置１０に送

信するなどの正当判定時の処理をおこなう（ステップＳ６０６）。

【００７３】

これとは反対に、正当アクセスのパターンのいずれにも該当しないものと判定された場合には（ステップＳ６０２否定）、このＨＴＴＰリクエストを見積部３２に受け渡し、上記実施の形態１または２によるフィルタリング処理と同様の処理をおこなう（ステップＳ６０３～６０８）。

【００７４】

すなわち、リクエストフィルタ７０の見積部３２は、ＨＴＴＰリクエストの正当性を見積もり（ステップＳ６０３）、判定部３４は、ＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡すか否かを判定する（ステップＳ６０４）。

【００７５】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップＳ６０４肯定）、リクエストフィルタ７０の送信部３５は、ＨＴＴＰリクエストをプロセス間通信によりＷｅｂサーバ４０に受け渡し（ステップＳ６０５）、Ｗｅｂサーバ４０は、ＨＴＴＰリクエストに応じた情報をクライアント装置１０に送信するなどの正当判定時の処理をおこなう（ステップＳ６０６）。

【００７６】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップＳ６０４否定）、リクエストフィルタ７０の送信部３５は、ＨＴＴＰリクエストのＷｅｂサーバ４０への受け渡しを拒絶し（ステップＳ６０７）、リクエストフィルタ７０の各部は、不正リクエストの破棄、格納媒体３６ｂへの格納、外部装置５０への通報などの不正判定時の処理をおこなう（ステップＳ６０８）。

【００７７】

上述してきたように、本実施の形態３によれば、画像ファイルを要求するＨＴＴＰリクエストのような要求の割合は高いが攻撃性は極めて低いものについては、見積部３２および判定部３３による処理を省いて迅速な処理をおこなうことができるとともに、パスワードファイルやＷｅｂサーバ４０上に存在しないファイ

ルを要求するＨＴＴＰリクエストのような攻撃性が高いものについては、見積部３２および判定部３３による処理をおこなって、かかる攻撃を有効に防御することができる。

【００７８】

なお、本実施の形態１～３では、クライアント装置１０からのＨＴＴＰリクエストをフィルタリングする場合について説明したが、本発明はこれに限定されるものではなく、ＦＴＰ（File Transfer Protocol）、ｔｅｌｎｅｔ、コンソールなど、クライアント装置１０からＷｅｂサーバ４０に入力されるあらゆる情報をフィルタリングする場合に同様に適用することができる。

【００７９】

また、本実施の形態１～３では、フィルタリング装置としてのリクエストフィルタ３０、７０をサーバ装置４０、６０に設けた場合について説明したが、本発明はこれに限定されるものではなく、例えば、それぞれのクライアント装置側にリクエストフィルタを設けたり、一つのリクエストフィルタにより複数のＷｅｂサーバを防御するなど、クライアント装置とＷｅｂサーバとの間にリクエストフィルタが介在するあらゆるシステム構成において同様に適用することができる。

【００８０】

なお、本実施の形態１～３で説明したフィルタリング方法は、あらかじめ用意されたプログラムをパーソナル・コンピューターやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フロッピーディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

【００８１】

（付記１）クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベ

ースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積手段と、

前記見積手段による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定手段と、

を備えたことを特徴とするフィルタリング装置。

【００８２】

（付記２）前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記判定手段は、前記見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記１に記載のフィルタリング装置。

【００８３】

（付記３）前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記判定手段は、前記見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記１に記載のフィルタリング装置。

【００８４】

（付記４）前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースと、前記見積手段による正当性の見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記１、２ま

たは３に記載のフィルタリング装置。

【００８５】

（付記５）所定の外部送信ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する外部送信手段をさらに備えたことを特徴とする付記１～４のいずれか一つに記載のフィルタリング装置。

【００８６】

（付記６）所定の格納ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する格納手段をさらに備えたことを特徴とする付記１～５のいずれか一つに記載のフィルタリング装置。

【００８７】

（付記７）所定の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新する更新手段をさらに備えたことを特徴とする付記１～６のいずれか一つに記載のフィルタリング装置。

【００８８】

（付記８）クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス要求のみを受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

を含んだことを特徴とするフィルタリング方法。

【００８９】

（付記９）前記見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要

求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記判定工程は、前記見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記８に記載のフィルタリング方法。

【００９０】

（付記１０）前記見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記判定工程は、前記見積工程により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記８に記載のフィルタリング方法。

【００９１】

（付記１１）前記見積工程による正当性の見積もりの前に、前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定工程をさらに含み、前記見積工程は、前記事前判定工程により正当アクセスのパターンに該当しないもの判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記８、９または１０に記載のフィルタリング方法。

【００９２】

（付記１２）所定の外部送信ルールに基づいて、前記判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する外部送信工程をさらに含んだことを特徴とする付記８～１１のいずれか一つに記載のフィルタリング方法。

【００９３】

（付記１３）所定の格納ルールに基づいて、前記判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する格納工程

をさらに含んだことを特徴とする付記８～１２のいずれか一つに記載のフィルタリング方法。

【００９４】

（付記１４）所定の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新する更新工程をさらに含んだことを特徴とする付記８～１３のいずれか一つに記載のフィルタリング方法。

【００９５】

（付記１５）前記付記８～１４のいずれか一つに記載された方法をコンピュータに実行させるプログラム。

【００９６】

【発明の効果】

以上説明したように、請求項１、８または９の発明によれば、サーバに対する不正アクセスのパターンを格納した不正パターンデータベースの不正アクセスのパターンおよび所定の見積ルールに基づいてアクセス要求の正当性を見積もり、この見積結果および所定の判定ルールに基づいてアクセス要求をサーバに受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみをサーバに受け渡すことができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができる。

【００９７】

また、請求項２の発明によれば、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、不正アクセスである旨が見積もられたアクセス要求をサーバに受け渡さないものと判定するとともに、正当アクセスである旨が見積もられたアクセス要求をサーバに受け渡すものと判定する

こととしたので、アクセス要求が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対しても迅速かつ確実にサーバを防御することができる。

【００９８】

また、請求項３の発明によれば、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、この算出された見積値と所定の閾値とを比較してアクセス要求をサーバに受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもある程度の幅を持ってサーバを防御することができる。

【００９９】

また、請求項４の発明によれば、正当性の見積もりの前に、サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、アクセス要求が正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定し、正当アクセスのパターンに該当しないもの判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなくサーバに受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

【０１００】

また、請求項５の発明によれば、所定の外部送信ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信することとしたので、不正アクセスに関する情報をサーバの管理者、フィルタリング装置の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に送信することができ、もってかかる管理者に対しサーバの保全対策を迅速に促すことができる。

【０１０１】

また、請求項６の発明によれば、所定の格納ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納することとしたので、格納媒体に格納された不正アクセスに関する情報を分析することなどができ、もってサーバの更なる保全対策を講じることができる。

【０１０２】

また、請求項７の発明によれば、所定の更新ルールに基づいて、不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新することとしたので、新たに発見された不正アクセスのパターンを不正パターンデータベースに登録することなどができ、もって日々進化する不正アクセスに対して機動的に対応することができる。

【図面の簡単な説明】

【図１】

本実施の形態１に係るクライアントサーバシステムの構成を示すブロック図である。

【図２】

不正リクエストＤＢに格納される情報の構成例を示す図である。

【図３】

本実施の形態１によるフィルタリングの処理手順を説明するフローチャートである。

【図４】

本実施の形態２によるフィルタリングの処理手順を説明するフローチャートである。

【図５】

本実施の形態３に係るクライアントサーバシステムの構成を示すブロック図である。

【図６】

本実施の形態３によるフィルタリングの処理手順を説明するフローチャートで

ある。

【符号の説明】

１　ネットワーク

１０　クライアント装置

１１　Ｗｅｂブラウザ

２０、６０　サーバ装置

３０、７０　リクエストフィルタ

３１　受信部

３２　見積もり部

３２ａ　見積ルール

３３　不正リクエストＤＢ

３４　判定部

３４ａ　判定ルール

３５　送信部

３６　ログ管理部

３６ａ　管理ルール

３７　外部通報部

３７ａ　通報ルール

３８　外部情報取得部

３８ａ　取得ルール

３９　更新部

３９ａ　更新ルール

４０　Ｗｅｂサーバ

５０　外部装置

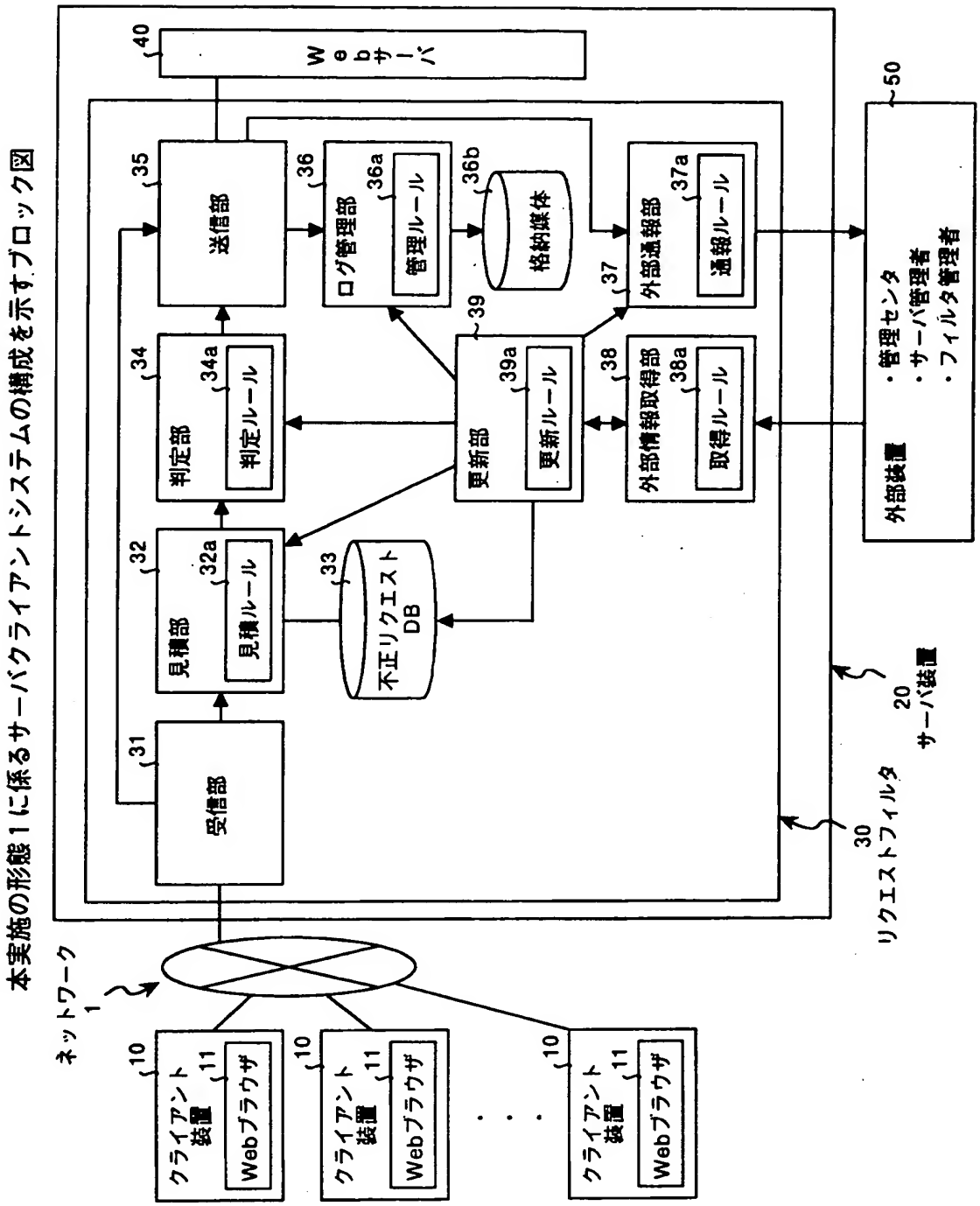
７１　事前判定部

７１ａ　事前判定ルール

７２　正当リクエストＤＢ

【書類名】　　図面

【図１】

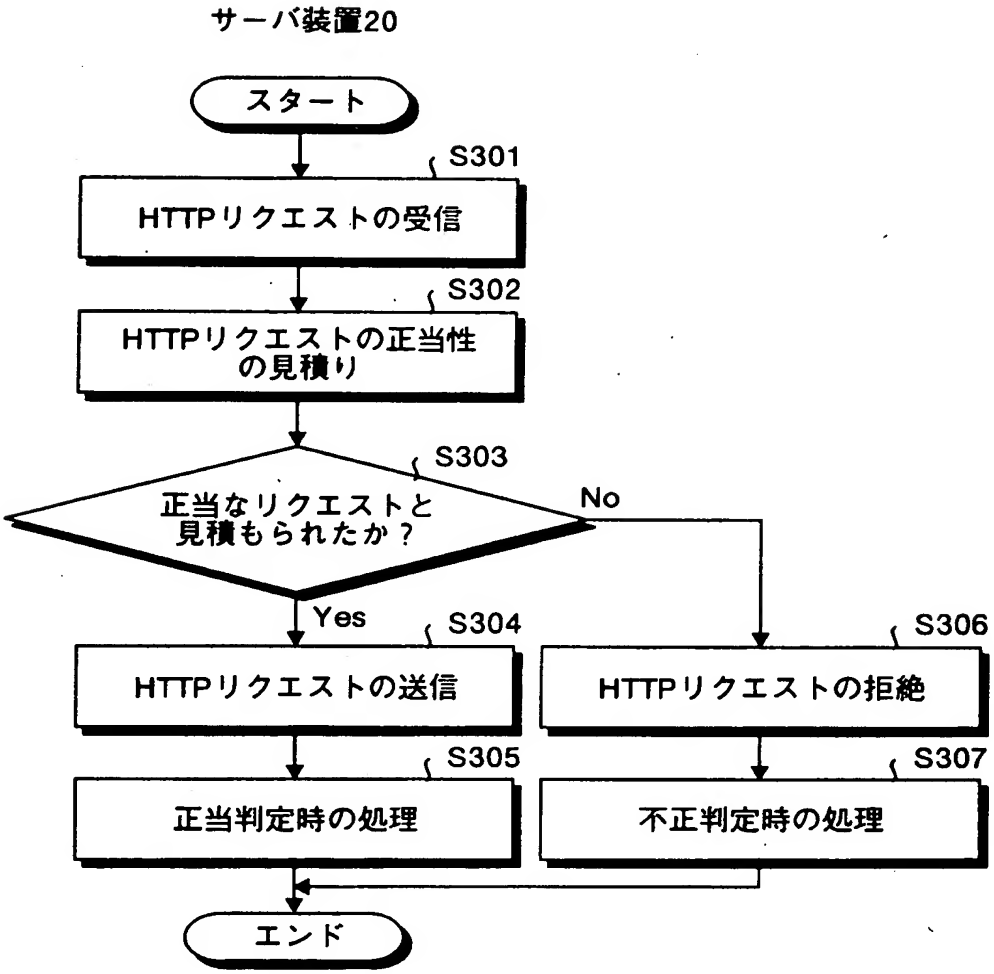

本実施の形態１に係るサーバクライアントシステムの構成を示すブロック図
ネットワーク
1
クライアント装置
10
Webブラウザ
11
受信部
31
見積部
32
見積ルール
32a
不正リクエストDB
33
判定部
34
判定ルール
34a
送信部
35
ログ管理部
36
管理ルール
36a
格納媒体
36b
外部通報部
37
通報ルール
37a
外部情報取得部
38
取得ルール
38a
更新部
39
更新ルール
39a
Webサーバ
40
リクエストフィルタ
30
サーバ装置
20
外部装置
50
・管理センタ
・サーバ管理者
・フィルタ管理者

不正リクエストDBに格納される情報の構成例を示す図

形式言語パターン	意味
URL=<//	URLの先頭が“//”と一致するリクエストを却下。
CGI==phf ARG=<Qname=root%OA	CGI名が“phf”であり、且つそのある引数の先頭が“Qname=root%OA”と一致するリクエストを却下。
URL<>..¥..¥..¥..	URLに“..¥..¥..¥..”が含まれるリクエストを却下。
CGI>=.htr	CGI名の末尾が、“.htr”と一致するリクエストを却下。 すなわち、CGIが拡張子“.htr”を有するリクエストを却下。

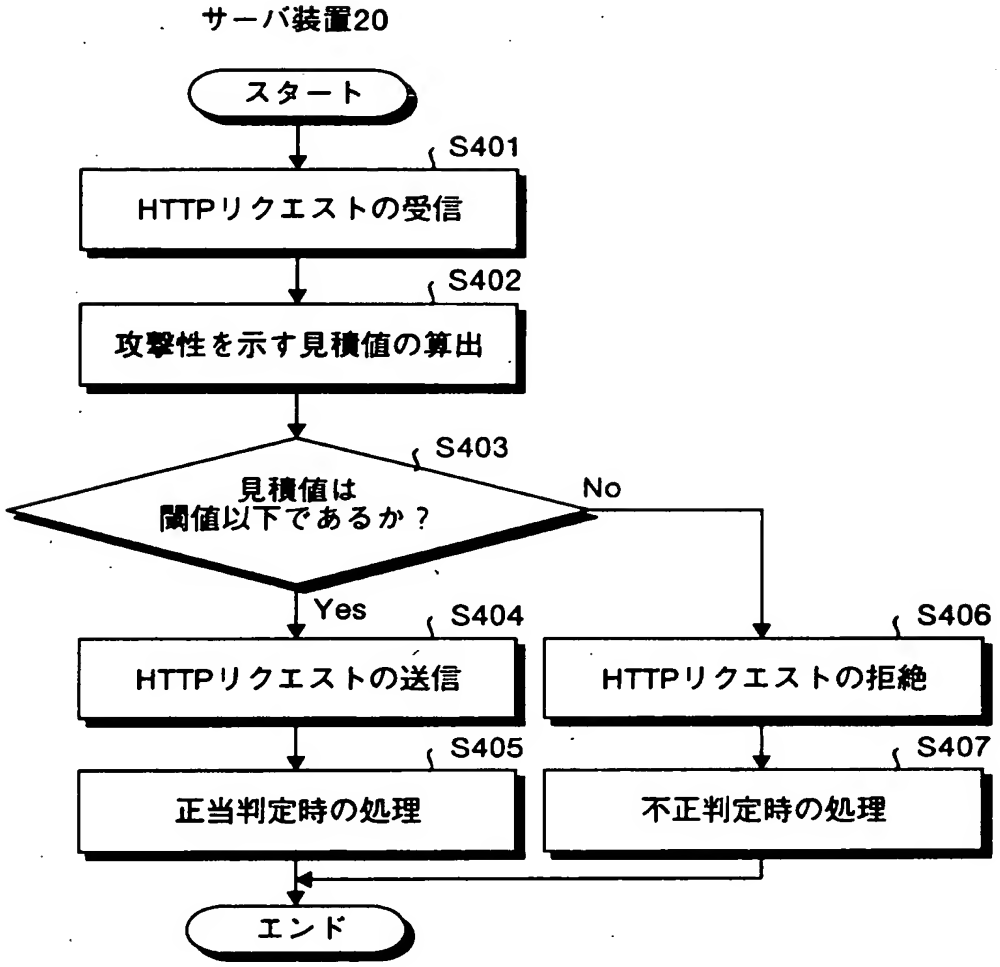
【図３】

本実施の形態１によるフィルタリングの処理手順を示すフローチャート

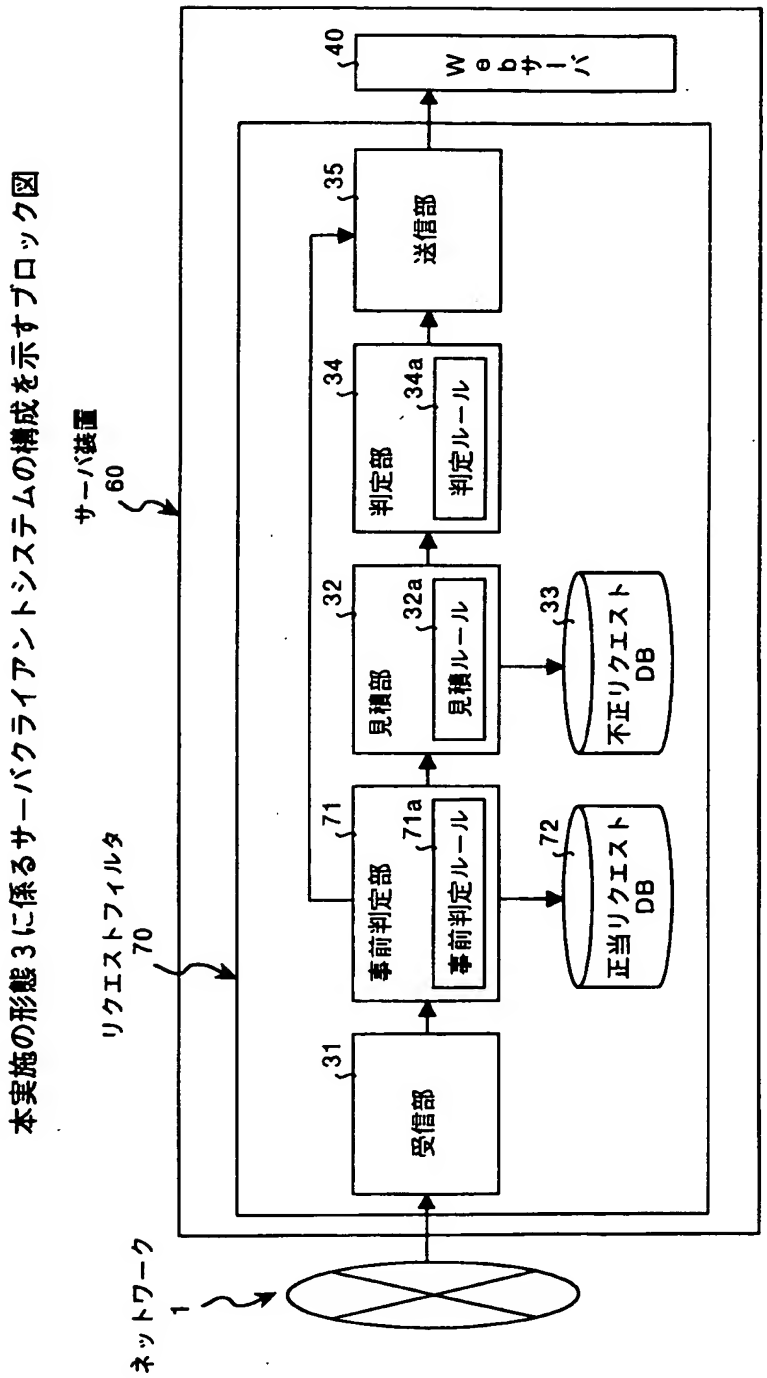


【図４】

本実施の形態２によるフィルタリングの処理手順を示すフローチャート

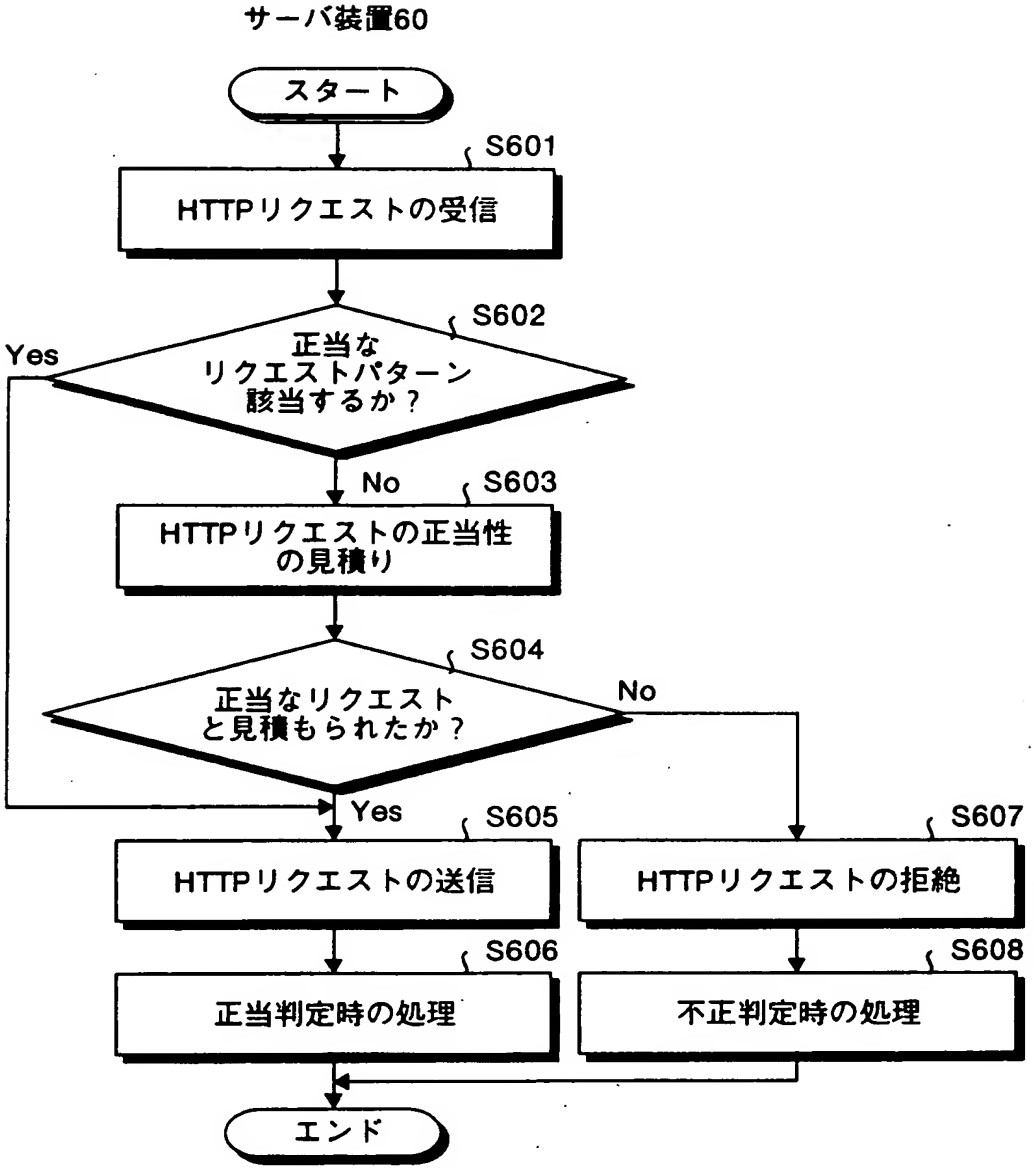


【図５】


本実施の形態３に係るサーバクライアントシステムの構成を示すブロック図
ネットワーク
1
サーバ装置
60
リクエストフィルタ
70
受信部
31
事前判定部
71
事前判定ルール
71a
正当リクエストDB
72
見積部
32
見積ルール
32a
不正リクエストDB
33
判定部
34
判定ルール
34a
送信部
35
Webサーバ
40

【図６】

本実施の形態３によるフィルタリングの処理手順を示すフローチャート



【書類名】　　要約書

【要約】

【課題】　不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御すること。

【解決手段】　Ｗｅｂサーバ４０に対する不正アクセスのパターンを格納した不正リクエストＤＢ（データベース）３３と、不正リクエストＤＢ３３に格納された不正アクセスのパターンおよび所定の見積ルール３２ａに基づいてクライアント装置１０からのアクセス要求の正当性を見積もる見積部３２と、見積部３２による見積結果および所定の判定ルール３４ａに基づいてアクセス要求をＷｅｂサーバ４０に受け渡すか否かを判定する判定部３４とを備える。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社